(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 March 2002 (14.03.2002)

PCT

(10) International Publication Number
WO 02/21283 A1

(51) International Patent Classification[7]: G06F 12/14, H04L 9/00

(21) International Application Number: PCT/AU01/01121

(22) International Filing Date:
5 September 2001 (05.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 9931 6 September 2000 (06.09.2000) AU

(71) Applicant *(for all designated States except US)*: **SANCTUARY SYSTEMS** [AU/AU]; P.O Box 1172, Bentley DC, Perth, Western Australia 6983 (AU).

(72) Inventors; and

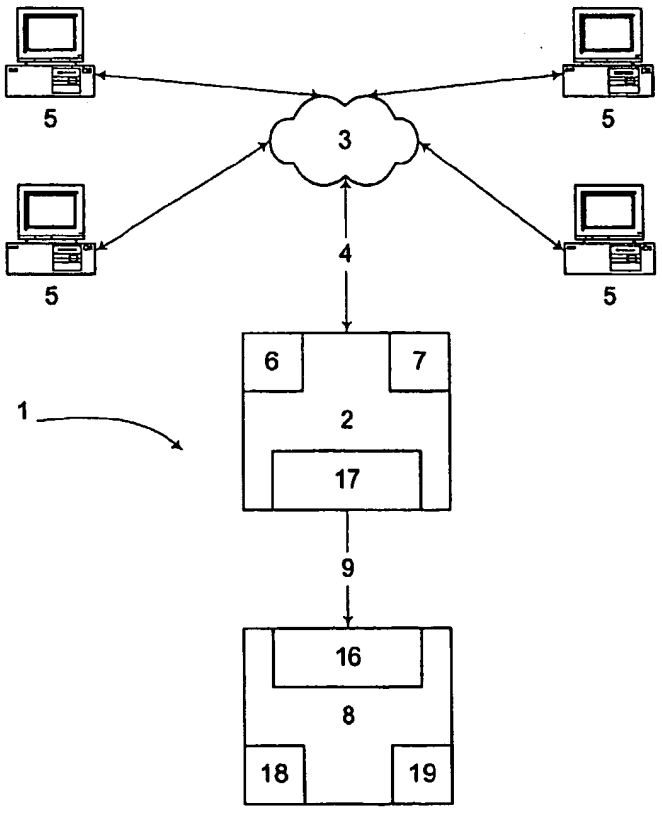
(75) Inventors/Applicants *(for US only)*: **MORRIS, John** [AU/AU]; CIIPS, University of Western Australia, Department of Electrical and Electronic Engineering, Stirling Highway (AU). **LEE, Gareth** [AU/AU]; CIIPS, University of Western Australia, Department of Electrical and Electronic Engineering, Stirling Highway, Nedlands, Western Australia 6009 (AU).

(74) Agent: **WRAY & ASSOCIATES**; Suite 6, Business Centre, 2A Brodie Hall Drive, Bentley, Western Australia 6102 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR TRANSMITTING AND STORING SENSITIVE DATA



(57) Abstract: A secure storage system for storing sensitive data out of reach of hackers. The system involves a data storage system 8 that is coupled to server 2 which receives data from remote terminals 5. When sensitive data is received from the terminals 5, the server 2 forwards the sensitive data to the storage system 8 by means of a one-way communications link 9. The link 9 allows a sensitive data packet to be sent in one direction only from the server 2 to the storage system 8 which in turn returns an acknowledgement packet to the server 2. The sever 2 and the storage system 8 can be linked by several links 9 and more than one storage system 8 can be coupled to the server 2. The sensitive data can be encrypted, interleaved with dummy data or split between several links 9 to be forwarded for storage.

WO 02/21283 A1

SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

"SYSTEM AND METHOD FOR TRANSMITTING AND STORING SENSITIVE DATA"

FIELD OF THE INVENTION

The present invention relates to a system and method for transmitting and storing data – particularly sensitive data – transmitted over communications networks, particularly, although not exclusively, public networks such as the Internet.

BACKGROUND ART

With the advent of improved data communication, computers are able to transmit and receive information between each other over long distances – commonly over networks, and often publicly accessible networks such as the Internet.

The Internet is a publicly accessible network to which millions of computers are connected. Typically, a user with a terminal, such as a Personal Computer, connects, via the Internet, to a server provided by his Internet Service Provider (ISP), and from there to one of many servers provided by a variety of companies, organisations, or individuals, to access, and sometimes download, information. A common application on the Internet is the provision of electronic retailing, wherein retailers provide information on products, which a user, or client can access, and then, very often, purchase directly. As with many applications of the Internet, it is desirable that any one user, with a computer, may access a server system that is operated by a retailer. For these applications, it is necessary for the server system to supply information - on request - to any computer coupled to the network, and to receive information from other computers. For example, an electronic retailer will need to supply product information to a potential client and, if the client wishes to purchase products offered, to receive information back from the client. The product information may be extensive and involve large amounts of text, images or sound. The information supplied by the client may contain sensitive information such as names, addresses and credit card numbers.

Since the server system needs to be accessed by any terminal on the public network, it needs to be open to the whole network and experience has shown that it is not possible to make such an open system entirely secure from intrusion - where unauthorised persons gain access to sensitive information. Systems involved in electronic commerce have been particularly vulnerable to attacks in which intruders are searching for credit card numbers. Loss of credit card numbers is just one example of a situation where an organization operating a server may be vulnerable to large damage claims if an intruder successfully obtains data, which can be used for fraudulent purposes.

The provision of credit card numbers during an on-line transaction is not the only situation where sensitive information is transmitted over the Internet. Service providers, such as taxation advisers and medical practitioners may receive confidential financial, medical or other personal information over the Internet. Thus, there is a general need for a system that offers a secure system for storing such information.

DISCLOSURE OF THE INVENTION

Throughout the specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

According to the present invention, there is provided a system for transmitting and storing data received from a terminal, the system comprising:

a data handling means arranged to receive data from the terminal;

and a data storage means coupled to the data handling means by at least one one-way communications channel arranged to transmit data in one direction from the data handling means to the data storage system;

the data handling means being operable to forward the received data to the data storage means via the at least one communications channel, the data storage means being operable to receive the data from the data handling means for storage in the storage means.

Preferably, the data handling means is operable to transmit the data to the data storage means within a data packet, the data storage means being operable to transmit, in response to a received data packet, an acknowledgement packet to the data handling means along the one-way communications channel, said acknowledgement packet being arranged not to contain the data.

Preferably, the data storage means is operable to generate an acknowledgement package containing a one-way hash function to verify the integrity of the received data packet.

Preferably, the data storage means is coupled to the data handling means by multiple one-way communications channels.

Preferably, the system further comprises multiple data storage means, each being coupled to the data handling means by one or more one-way communications channels.

Preferably, the data handling means includes encryption means operable to encrypt data prior to transmission along the one-way communication channel, and the data storage includes decryption means operable to decrypt the received encrypted data.

Preferably, the data is encrypted using public key encryption, and the data is decrypted using a private key held in the decryption means.

Preferably, the data handling means is operable to transmit the data along the at least one one-way communication channel interleaved with randomly generated data.

Preferably, the data handling means is operable to transmit the data along the at least one one-way communication channel embedded within a series of data packets,

Preferably, the system includes multiple one-way communication channels, wherein the data handling means is operable to transmit the data sequentially along the communications channels

Preferably, the data handling means is operable to transmit the data along randomly selected communications channels.

Preferably, the data handling means is operable to transmit the data along all communications channels, with only portions of the data on any single channel,

Preferably, the data handling means is operable to transmit the data along all communications channels, with one channel transmitting the actual data, the others bogus data.

Preferably, the data handling means is operable to transmit encrypted data directly to the data storage means, the data storage means including decryption means operable to decrypt the encrypted data, the data storage means being further operable to transmit, in response to the received data, an acknowledgment packet to the data handling means along the one-way communications channel, the acknowledgment packet being arranged not to contain the data.

Preferably, the acknowledgement packet contains flags indicating whether the encrypted data was valid.

According to another aspect of the present invention, there is provided a method for transmitting and storing data received from a terminal by a data handling means, said method comprising the steps of: providing a data storage means; providing at least one one-way communications channel between the data handling means and the data storage means arranged to permit transmission of data in one way only from the data handling means to the data storage means;

the data handling means transmitting the received data to the data storage means for storage therein via the at least one one-way communication channel.

Preferably, the data is transmitted within a data packet, and an acknowledgement packet is sent, from the data storage means to the data handling means, along the one-way communications channel, in response to a received data packet, the acknowledgement packet being arranged not to contain the data.

Preferably, the acknowledgement package contains a one-way hash function to verify the integrity of the received data packet.

Preferably, the data is encrypted prior to transmission along the one-way communication channel, and is decrypted upon receipt by the data storage means.

Preferably, the data is encrypted using public key encryption, and the data is decrypted using a private key.

Preferably, the data is transmitted along the at least one one-way communication channel interleaved with randomly generated data.

Preferably, the data is transmitted along the at least one one-way communication channel embedded within a series of data packets.

Preferably, the method includes the step of providing multiple one-way communication channels, wherein the one-way communication channel along which a data packet is to be transmitted is sequentially selected.

Preferably the method includes the step of providing multiple one-way communications channels, wherein the one-way communication channel along which a data packet is to be transmitted is randomly selected.

Preferably the method includes the step of providing multiple one-way communications channels, wherein the data is transmitted along all communications channels, with only portions of the data on any single

The invention has the advantage that sensitive information transmitted over an insecure network to a data handling system – such as a server for an Internet site – is stored remotely in a data storage system coupled to the data handling system by means of a communications channel that allows the sensitive data to be transmitted in only one direction – namely from the data handling system to the data storage system – and not the other direction, so that the data is stored out of reach of a potential fraudulent user.

In addition, the use of one or more means of transmitting the data from the data handling means to the data storage means further increases the security of the system, and makes it even less likely that someone would be able to gain access to the sensitive information.

With the system of the present invention, even if a fraudulent user were to gain access to the data handling system, he would have to:

- first determine that a remote data storage system was coupled to the data handling system
- then determine which communications channel or channels are being used for communication to the data storage system
- then devise a method for observing the data packets being transmitted on those channels
- if cryptography is used, obtain the private key used for decrypting transactions (if public key cryptography is used, this is stored on the data storage systems, and one must rely on trial and error - with a very low probability of success - to find the correct key)
- if multiple channels are being used, determine either which channel is being used for valid transactions, or

- when transactions are detected and decrypted on multiple channels, determine which of these transactions are bogus transactions and which contain useful data

- when data is split among different packets of data, determine which parts of these packets comprise the real data; and

- assuming that an intruder were able to succeed in all of these steps and successfully obtain one set of sensitive data, then, since the data handling system does not need to use the same method or channels for the next transaction, the intruder would have to run through the whole procedure again. This will make it impractical for an intruder to insert automatic snooping tools into the server to collect useful information (as distinct from randomly generated bogus data).

As mentioned above, the data handling means may be arranged to transmit encrypted data directly to the data storage means, where this is decrypted. In this case, the acknowledgement packet may contain flags indicating whether the encrypted data was valid. This arrangement is particularly advantageous where the remote terminal encrypts the data prior to transmission to the data handling system, such as by using public key cryptography. The data handling means will then never need to decrypt the data received from the remote terminal.

In this case, the sensitive data is never available on the data handling system i.e. the part vulnerable to external attack, in decrypted or plain text form.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described, by way of example only, with reference to the accompanying drawings, of which:

Figure 1 is a schematic illustration of a first embodiment of the invention;

Figure 2 is a schematic illustration of a second embodiment of the invention;

Figure 3 is a schematic illustration of a third embodiment of the invention; and

Figures 4a and 4b are schematic illustrations of a data packet and acknowledgement packet respectively.

BEST MODE(S) FOR CARRYING OUT THE INVENTION

A communications and information storage system 1 comprises a data handling system, such as a server 2 which may be connected to a public communications network 3, such as the Internet, via a publicly accessible communications channel 4. The server 2 includes a processor 6 and memory 7 for storing information, for example, in a database.

Remote terminals 5, operated by users, are also connected to the public communications network 3. The remote terminals 5 can send information to, and receive information from, the server 2 over the public communications network 3.

The operation and construction of such networks is well known to persons skilled in the art, and, in so far as it is not relevant to the present invention, need not be described in any further detail herein.

The communications and information storage system also includes a data storage system 8 connected to the server 2 by means of a one-way communications channel 9.

For the avoidance of doubt, the term "one-way", as used with regard to the communication channels discussed herein, refers to the fact that it is the data which can only flow in one direction – namely from the server 2 to the data storage system 8, and not in the other direction. The data storage system 8 is also a server that also includes a processor 19, and a memory 18 for storing data transmitted along the one-way communications channel 9. The data is received from a remote terminal 5 by the processor 6, and is transmitted under control of the processor 6, to the data storage system 8, but cannot be transmitted back to the server 2 from the data storage system 8. This is achieved by means of

protocol management software in the data storage system 8 that permits communication only in one direction along the one-way channel, namely from the server 2 to the data storage system 8, and not in the other direction.

The data storage system 8, and the server 2 can be any suitable server configured to operate in accordance with the invention. As such, and in so far as it is not relevant to the present invention, the servers and their operation need not be described in any further detail herein.

The server 2 may be operated, for example, by an electronic retailer and contain databases of product information which is supplied to potential clients who access the server 2 via a remote terminal 5, using a web browser – again, as is well known to persons skilled in the art. At some point – for example, when purchasing an item, the client may need to send sensitive information to the server 2, which is sent, via the public network 3, to the server 2. This sensitive information could include confidential details, which the client does not want to be made publicly available. Rather than retain the sensitive information in its own databases in the memory 7, the server 2 transmits the sensitive information immediately to the data storage system 8 using the one-way communication channel 9.

Because the data storage system 8 is not connected to the public network, remote users of the public network 3 are unable to gain access to it, to, for example, to subvert the protocol management software, which prevents sensitive data from being transmitted from the data storage system 8 back to the server 2.

In a second embodiment of the invention, two one-way communications channels 9, 10 are used to link the server 2 and the data storage system 8. Both channels 9, 10 only transmit data in one direction – namely from the server 2 to the data storage system 8.

In a third embodiment, the server 2 is connected to a first and second data storage systems 11,12 – each data storage system 11, 12 being linked by their own respective one-way communications channel 13, 14.

As a further alternative, more than two one-way channels could be used, with either a single data storage system, or there could be provided a data storage system for each one-way channel – or combinations thereof.

The communications protocol between the server 2 and the data storage system 8 consists of data packets 21 - such as the one illustrated in fig 4a - and acknowledgement packets 15 only - such as the one illustrated in fig 4b.

A typical data packet 21 may include a transaction identifier 21a, information on the credit card holder's name 21b, credit card number 21c, expiry date 21d, and amount 21e, and 32-bit portion of check/identification data 21f.

A typical acknowledgement packet 15 consists of a transaction identifier 15a and message digest 15b that verifies the integrity of the data packet 21, by advising the server 2 that the data packet 21 is complete and that all constituent parts are correct.

The communications software on server 2 transmits data packets and reads acknowledgement packets. The communications software on data storage system 8 receives data packets and transmits acknowledgement packets. When the sensitive data reaches the information data storage system 8 it may be stored in files or databases or other conventional means. The sensitive data may then be accessed using a terminal that is connected directly to the data storage system 8 and not to any public network, or connected via a secure private network.

The process by which sensitive data is handled by the server 2 and the data storage system 8 is as follows:

I. the server 2 sends some information (*eg* specifications of some product) to a remote terminal, in response to a request from the remote terminal 5;

II. the remote terminal 5 responds by sending data – including sensitive information - back to the server 2 (*eg* name, address and credit card number for a potential purchase). Normally the message containing the sensitive information will be

encrypted using commonly known techniques as it is transmitted through the public network. This data – including the sensitive information – is temporarily stored in the memory 7 until it is transmitted to the data storage system 8;

III. immediately upon receiving the sensitive information, the server 2 decides which one-way channel (or channels) 9, 10, 13, 14 to use, decrypts the information to check it for completeness, then immediately encrypts the sensitive portions of the information again, and transmits the data along with a transaction identifier 21a – in the form of a data packet 15 - to the data storage system 8;

IV. the data storage system 8 then sends a short acknowledgement packet 15 containing the transaction identifier 15a back to the server 2 in response to the received data. The message digest 15b is a one-way hash function. One-way hash functions digest the contents of a specific message without providing a way to reconstruct the message from the digest. Any suitable hash function could be used, for example, the Secure Hash Standard algorithm as disclosed in the publication: National Institute of Standards and Technology, NIST FIPS PUB 180, "Secure Hash Standard", U.S. Department of Commerce, May 1993. The term "digest", "message digest", and "one-way hash function" are synonymous.

V. the server 2 waits for the acknowledgement from 15 the data storage system 8 and then erases the sensitive data from its memory 7 and transmits an acknowledgement to the remote terminal 5.

Thus the sensitive data is available on the server 2 in unencrypted form for the minimum possible time – that is the time in step (III) when the data is being checked for completeness.

In a variation of this procedure, encrypted data that is received from the remote terminal 5 can immediately be sent to the selected data storage system 8 without decryption. The data storage system 8 can then decrypt it, check it for completeness, and send an acknowledgement. This acknowledgement will contain only flags indicating whether the sensitive data was complete or not. With

this variation, the sensitive data is never available on the server 2 (the one vulnerable to intruder attack) in decrypted or plain text form.

In any of the embodiments described above, any or all of the following techniques can be used – at various times - to increase the security of the transmitted data:

(a) data is encrypted before transmission from the server 2 using an encryption means 17 – and is then decrypted upon receipt by the data storage system 8 using decryption means 16;

(b) if public key encryption - for example as defined by the RSA system, US Patent 4405829, 20th September, 1983, R L Rivest, A Shamir and L M Adleman - is used, then the private key is only held in the decryption means 16 on the data storage system 8 and thus not available within the server 2;

(c) actual data is interleaved with packets of dummy data containing randomly generated data which an intruder could mistake for genuine data;

(d) data may also be inserted into a number of full data packets in which most of the data is randomly generated bogus data used to make each transaction appear complete. A cryptographic technique could be applied to this task, known as "Secret Splitting", which creates N mutually independent random data packets, such that the original data packet can only be recovered by combining all N packets - see Bruce Schneier, "Applied Cryptography", Wiley and Assoc., 1996, Section 3.6, Page 70. An eavesdropper who obtained an incomplete set would be unable to recover any of the original data.

Where two or more one-way communication channels are used:

(e) the channel to be used to transmit a data packet is chosen sequentially. For example, one channel is chosen for the first data packet, and the second channel for the second data packet and so on. Where there are two one-way communications channels, then alternate channels could be used;

(f) the channel to be used to transmit a data packet is chosen randomly;

(g) where two channels are used, both channels are used with only parts of the sensitive data being sent on any single channel;

(h) a channel not used for sending actual data transmits suitably corrupted versions of the actual data.

Different combinations of some or all of techniques (a)-(h) can be used at various times. For example, one transaction is sent over one channel accompanied by dummy data on another channel and the next transaction is transmitted using two channels.

Where there are multiple one-way channels linking the server 2 and the one or more data storage systems 8, 11, 12, in step (iii) above, the server 2 can divide the data to be transmitted among the channels 9, 10, 13, 14. This need not be all of the available channels.

When the data is split between channels 9, 10, 13, 14, it may be sent as a number of short data packets, which are assembled at the respective data storage system 8, 11, 12 to recreate the full information.

The channels chosen for any step may vary from transaction to transaction.

In parallel with step of transmitting data to the data storage system 8, bogus data, randomly generated to look like a real transaction, could be sent along unused channels.

It will be understood to persons skilled in the art, that variations are possible within the scope of the present invention.

The Claims Defining the Invention are as Follows

1. A system for transmitting and storing data received from a terminal, the system comprising:

   a data handling means arranged to receive data from the terminal;

   and a data storage means coupled to the data handling means by at least one one-way communications channel arranged to transmit data in one direction only, from the data handling means to the data storage system;

   the data handling means being operable to forward the received data to the data storage means via the at least one communications channel, the data storage means being operable to receive the data from the data handling means for storage in the storage means.

2. A system as claimed in claim 1, wherein the data handling means is operable to transmit the data to the data storage means within a data packet, the data storage means being operable to transmit, in response to a received data packet, an acknowledgement packet to the data handling means along the one-way communications channel, said acknowledgement packet being arranged not to contain the data.

3. A system according to claim 1 or claim 2, wherein the data storage means is operable to generate an acknowledgement package containing a one-way hash function to verify the integrity of the received data packet.

4. A system as claimed in any preceding claim, wherein the data storage means is coupled to the data handling means by multiple one-way communications channels.

5. A system according to claim 4, comprising multiple data storage means, each being coupled to the data handling means by one or more one-way communications channels.

6. A system according to any preceding claim, wherein the data handling means includes encryption means operable to encrypt data prior to transmission along the one-way communication channel, and the data storage includes decryption means operable to decrypt the received encrypted data.

7. A system according to claim 6, wherein the data is encrypted using public key encryption, and the data is decrypted using a private key held in the decryption means.

8. A system according to any preceding claim, wherein the data handling means is operable to transmit the data along the at least one one-way communication channel interleaved with randomly generated data.

9. A system according to any preceding claim, wherein the data handling means is operable to transmit the data along the at least one one-way communication channel embedded within a series of data packets,

10. A system according to any preceding claim, including multiple one-way communication channels, wherein the data handling means is operable to sequentially select the one-way communication channel along which a data packet is to be transmitted.

11. A system according to any of claims 1 to 9, including multiple one-way communications channels, wherein the data handling means is operable to randomly select the one-way communication channel along which a data packet is to be transmitted.

12. A system according to any of claims 1 to 9, including multiple one-way communications channels, wherein the data handling means is operable to transmit the data along all communications channels, with only portions of the data on any single channel,

13. A system according to any of claims 1 to 9, including multiple one-way communications channels, wherein the data handling means is operable to

transmit the data along all communications channels, with one channel transmitting the actual data, the others bogus data.

14. A system according to claim 1, wherein the data handling means is operable to transmit encrypted data directly to the data storage means, the data storage means including decryption means operable to decrypt the encrypted data, the data storage means being further operable to transmit, in response to the received data, an acknowledgment packet to the data handling means along the one-way communications channel, the acknowledgment packet being arranged not to contain the data.

15. A system as claimed in claim 14, wherein the acknowledgement packet contains flags indicating whether the encrypted data was valid.

16. A method for transmitting and storing data received from a terminal by a data handling means, said method comprising the steps of: providing a data storage means ; providing at least one one-way communications channel between the data handling means and the data storage means arranged to permit transmission of data in one way only from the data handling means to the data storage means; the data handling means transmitting the received data to the data storage means for storage therein via the at least one one-way communication channel.

17. A method as claimed in claim 16, wherein the data is transmitted within a data packet, and an acknowledgement packet is sent, from the data storage means to the data handling means, along the one-way communications channel, in response to a received data packet, the acknowledgement packet being arranged not to contain the data.

18. A method according to claim 16 or claim 17, wherein the acknowledgement package contains a one-way hash function to verify the integrity of the received data packet.

19. A method according to any preceding claim, wherein the data is encrypted prior to transmission along the one-way communication channel, and is decrypted upon receipt by the data storage means.

20. A method according to claim 19, wherein the data is encrypted using public key encryption, and the data is decrypted using a private key.

21. A method according to any of claims 16 to 20, wherein the data is transmitted along the at least one one-way communication channel interleaved with randomly generated data.

22. A method according to any preceding claim, wherein the data is transmitted along the at least one one-way communication channel embedded within a series of data packets.

23. A method according to any of claims 16 to 22, including the step of providing multiple one-way communication channels, wherein the one-way communication channel along which a data packet is to be transmitted is sequentially selected.

24. A method according to any of claims 16 to 22, including the step of providing multiple one-way communications channels, wherein the one-way communication channel along which a data packet is to be transmitted is randomly selected.

25. A method according to any of claims 16 to 22, including the step of providing multiple one-way communications channels, wherein the data is transmitted along all communications channels, with only portions of the data on any single channel,

26. A method according to any of claims 16 to 22, including the step of providing multiple one-way communications channels, wherein the data is transmitted along all communications channels, with one channel transmitting the actual data, the others bogus data.

27. A method according to claim 16, wherein encrypted data is transmitted directly to the data storage means, encrypted data is decrypted by the data storage means, and an acknowledgment packet is transmitted to the data handling means along the at least one-way communications channel, in response to the received packet, the acknowledgment packet being arranged not to contain the data.

28. A method as claimed in claim 27, wherein the acknowledgement packet contains flags indicating whether the encrypted data was valid.

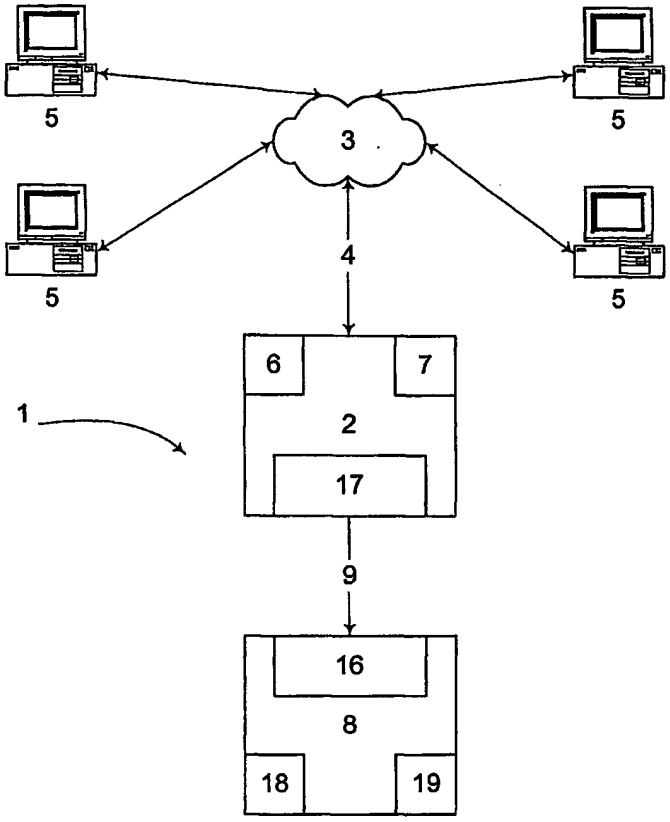


Figure 1

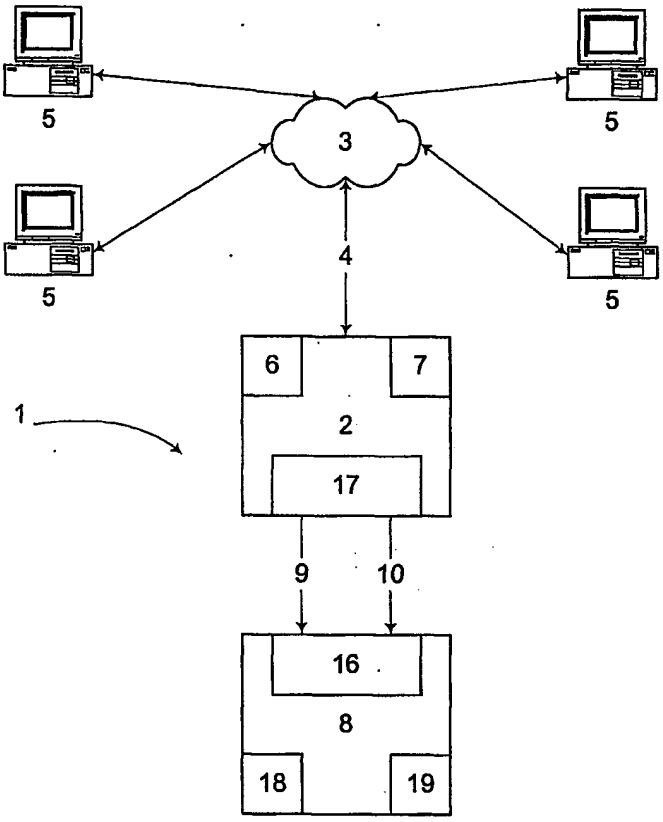


Figure 2

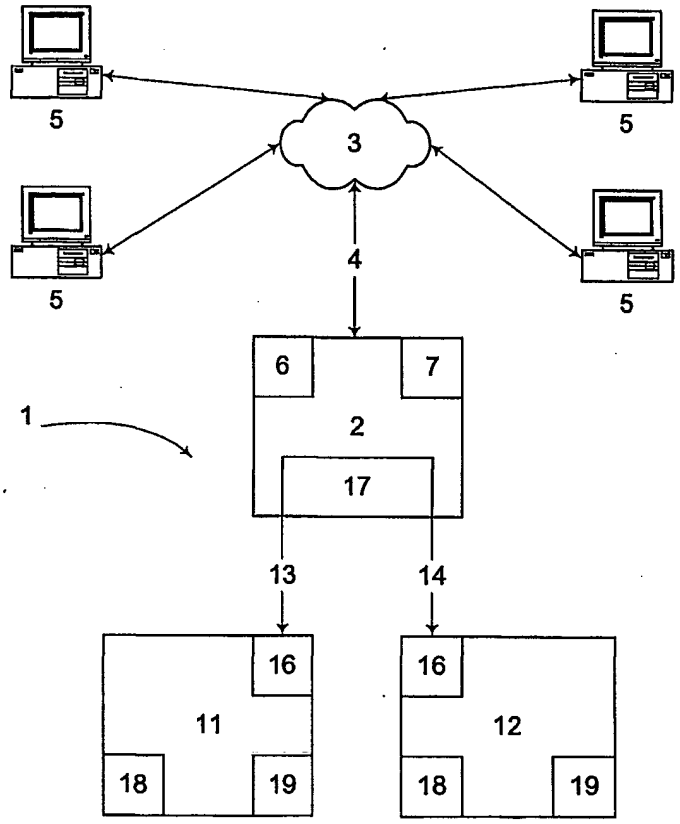


Figure 3

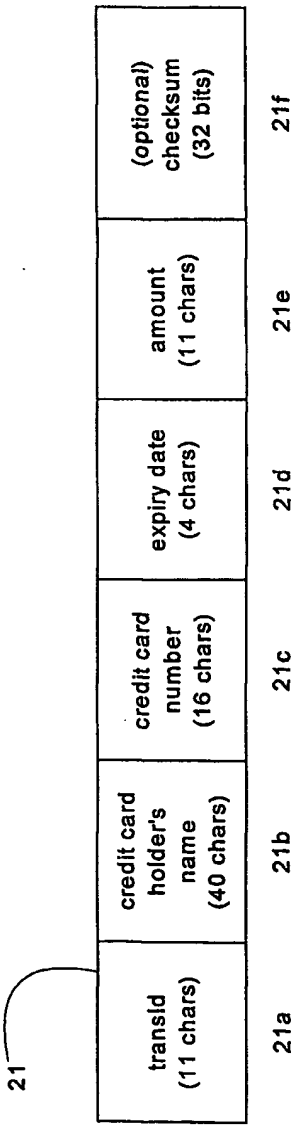


Figure 4a

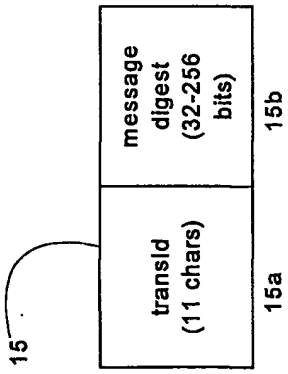


Figure 4b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/01121

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 12/14, H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT, USPTO Web Patent Database, Esp@cenet, "communication, one way, unidirection, memory etc"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4811277 A (MAY et al.) 7 March 1989 Figures 2 to 4 for example.	1,2,9,16,17,22
X	US 5630207 A (GITLIN et al.) 13 May 1997 Column 6 lines 7 to 16 for example.	1-4,5,9,16-18,22
X	US 5668803 A (TYMES et al.) 16 September 1997 Column 7 lines 61 to column 8 line 1 for example.	1,2,4,9,12,16,17,22,25
X	US 5727065 A (DILLON) 10 March 1998 Column 6 lines 11 to 25 for example.	1,9,16,22

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 October 2001	24 OCT 2001
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer P. THONG Telephone No : (02) 6283 2128

INTERNATIONAL SEARCH REPORT	International application No. PCT/AU01/01121

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/31908 A (CONSONANCE TECHNOLOGIES, INC) 2 June 2000 Column 5 lines 17 to 29 and column 9 lines 4 to 15 for example.	1,4,11,16,24
X	WO 00/49753 A (BROWNE, HENDRIK, A.) 24 August 2000 Page 15 line 25 to page 16 line 3 for example.	1,16
X	US 5247575 A (SPRAGUE et al.) 21 September 1993 Column 9 lines 20 to 22, lines 24 to 28 and 40 to 43 for example.	1,9,16,22

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/01121

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	4811277	EP	141659	WO	8502041		
US	5630207	EP	750284	JP	9009323		
US	5668803	AU	58080/90	CA	1310370	EP	405074
		CN	1096121	JP	3038133	US	5029183
		ZA	9300242	US	5837986	BR	9300173
US	5727065	NONE					
WO	200031908	AU	200015193	EP	1131908	NO	20012581
WO	200049753	AU	200035956	US	6272533		
US	5247575	AU	41882/89	EP	472521	WO	9002382

END OF ANNEX